The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
2/18/2010

SUBJECT:
Multiple Vulnerabilities Discovered in Mozilla Products Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in the Mozilla Firefox and Mozilla SeaMonkey applications which could allow remote code execution as well as cross domain scripting. Mozilla Firefox is a web browser used to access the Internet. Mozilla SeaMonkey is a cross platform Internet suite of tools ranging from a web browser to an email client. The Mozilla applications (Firefox and SeaMonkey) utilize the same framework to display application specific information (e.g. Web pages, emails, chats).

These vulnerabilities may be exploited if a user visits a webpage or opens a malicious file specifically crafted to take advantage of these vulnerabilities. Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

SYSTEMS AFFECTED:

Mozilla Firefox versions 3.5.7 and earlier
Mozilla SeaMonkey version 2.0.2 and earlier
Mozilla Thunderbird version 3.0.1 and earlier

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:

Multiple vulnerabilities have been discovered in Mozilla Firefox and Mozilla SeaMonkey. These vulnerabilities could allow an attacker to take complete control of an affected system or steal cookie-based authentication credentials. Details of these vulnerabilities are as follows:

Mozilla Firefox and SeaMonkey Remote Memory Corruption Vulnerability (MFSA 2010-02)
A vulnerability exists as a result of a memory corruption error that resides in the implementation of 'Web Workers' and the way it handles array data types when processing posted messages. An attacker can exploit this vulnerability if a user visits a specially crafted web page.

Mozilla Firefox Multiple Remote Memory Corruption Vulnerabilities (MFSA 2010-01)
Multiple vulnerabilities exist as a result of multiple memory-corruption errors that are contained in the browser engine. These vulnerabilities may be exploited if a user visits a specifically crafted web page.

Mozilla Firefox/Thunderbird/SeaMonkey HTML Parser Remote Code Execution Vulnerability (MFSA 2010-03)
A remote code execution vulnerability exists due to an error within the 'use-after-free' condition in the HTML parser of these applications. This issue arises when the applications incorrectly free used memory when insufficient space is available to process remaining input. This vulnerability may exploited if a user opens a specially crafted web page or opens a malicious email.

Mozilla Firefox and SeaMonkey SVG Document Cross Domain Scripting Vulnerability (MFSA 2010-05)
Mozilla Firefox and SeaMonkey are prone to a cross-domain scripting vulnerability. This vulnerability arises due to the way that the applications handle SVG documents that are referenced via the 'embed' tag with the 'type' attribute set to 'image/svg+xml'. SVG (Scalable Vector Graphics) is an XML language for sophisticated 2D graphics. Successful exploitation of this vulnerability could allow an attacker to steal cookie-based authentication credentials or to launch other attacks.

Mozilla Firefox and SeaMonkey 'showModalDialog' method Cross Domain Scripting Vulnerability (MFSA 2010-04)
A cross-domain scripting vulnerability exists when the application fails to properly enforce the same-origin policy. This issue exists when objects are passed to 'ShowModalDialog' and are readable even when the document comes from a different domain. This vulnerability can be exploited if a user visits a specially crafted web page.

Successful exploitation of the vulnerabilities identified above could result in an attacker gaining the same privileges as the logged on user or the theft of cookie-based authentication credentials. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

RECOMMENDATIONS:

The following actions should be taken:

- Install the Mozilla patches and upgrades immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Security Focus:
http://www.securityfocus.com/bid/38285
http://www.securityfocus.com/bid/38286
http://www.securityfocus.com/bid/38287
http://www.securityfocus.com/bid/38288
http://www.securityfocus.com/bid/38289

Mozilla:
http://www.mozilla.org/security/announce/2010/mfsa2010-01.html
http://www.mozilla.org/security/announce/2010/mfsa2010-02.html
http://www.mozilla.org/security/announce/2010/mfsa2010-03.html
http://www.mozilla.org/security/announce/2010/mfsa2010-04.html
http://www.mozilla.org/security/announce/2010/mfsa2010-05.html

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0160
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0159
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1571
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0162
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3988